A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER (DC3)

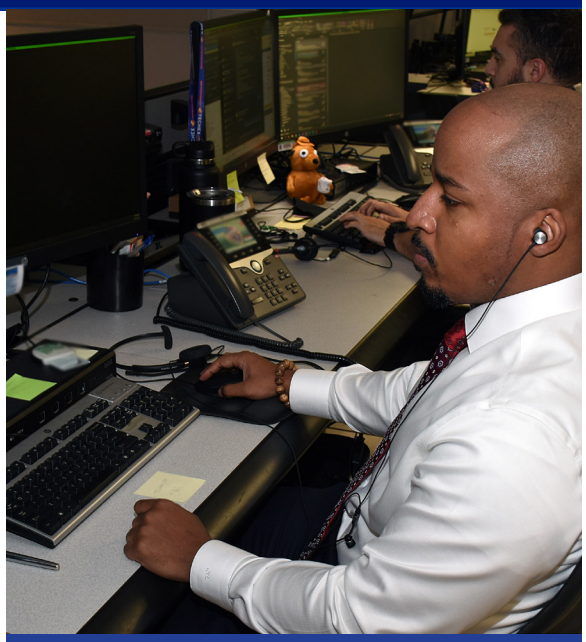
DoD—Defense Industrial Base Collaborative Information Sharing Environment

DCISE FACT SHEET

DoD-Defense Industrial Base Collaborative Information Sharing Environment (DCISE)—DCISE is the operational hub of DoD's Defense Industrial Base (DIB) Cybersecurity Program, focused on protecting intellectual property and safeguarding DoD content residing on or transiting through, contractor unclassified networks. The public-private cybersecurity partnership provides: a collaborative environment for crowd-sourced threat sharing at both unclassified and classified levels, Cleared Defense Contractor (CDC) cyber resilience analyses, and Cybersecurity-as-a-Service pilot offerings. DCISE performs cyber threat analysis and diagnostics, offers mitigation and remediation strategies, provides best practices, and conducts analyst-to-analyst exchanges with DIB participants ranging in size from small to enterprise-sized companies.

DC3/DCISE is the reporting and analysis hub for implementation of 10 US Code Sections 391 and 393 regarding the reporting of certain types of cyber incidents by CDCs, and the related Defense Federal Acquisition Regulation Supplement (DFARS 252.204-7012). Cyber incidents outlined in the DFARS are submitted to DC3/DCISE as mandatory reports; however, all other cyber activity can be reported voluntarily.

- Rated as Capability Maturity Model Integration for Services (CMMI-SVC) Maturity Level 3
- Collaborative partnership with over 885 CDCs and U.S. Government (USG) agencies
- Shared over 519,000+ actionable, non-attributable (to submitting source) indicators
- Provided over 78,000+ hours of no-cost forensics and malware analysis for DIB Partners
- Disseminated 12,500+ cyber threat reports for both DIB and USG consumption (DIB partners may access DCISE reporting via their DIBNET accounts and USG members can access via SIPRNet Intelshare)
- Operates 24/7/365 DCISE support hotline (1-877-838-2174) to assist submitters and DIB and USG Partners



" The threat is real. By sharing our findings, we can reduce risk together. "

—DCISE

DoD CYBER CRIME CENTER

DCISE@dc3.mil 410-981-0104 | www.dc3.mil | info@dc3.mil @DC3DCISE · @DC3Forensics DC3 Cyber Crime Center

DCISE CAPABILITIES

Analytics Division (AD): AD conducts analysis on cyber activity submitted by DIB Partners, DoD, and other USG agencies to develop a complete understanding of known or potential threats to unclassified DoD information on or transiting DIB systems and networks. AD also analyzes aggregate data from DIB Partner incident reports to produce technical analysis products, presentations, and other threat mitigation resources. The Division collaborates with liaison officers from USG agencies to create and maintain technical and multi-source threat profiles.
The Analytics Division is comprised of two branches:

1. **Tactical Operations:** Conducts daily processing of voluntary and mandatory incident reports, as well as malware analysis, Customer Response Forms (CRFs), CRF Supplements, and partner engagement.
2. **Applied Research:** Handles mid- to long-term analysis, resulting in the following threat products: Threat Activity Reports (TARs), Cyber Targeting Analysis Reports (CTARs), Alerts, Warnings, Threat Information Products (TIPs), and other threat-based analyses. To share valuable information with the DIB, this branch requests the downgrade and release of classified information derived from USG sources. Such information is shared via DCISE Cyber Threat Bulletins (CTBs) and Advisories.

Expanded Offerings and Projects (XOP) Division: XOP researches services that support DIB Partners in protecting DoD information. These services are offered as pilots to the DIB Partnership. The pilots range from services to capabilities and are intended to encompass all concepts, technologies and processes within cybersecurity. XOP was created because of the need for evolving solutions based on the ever-changing cybersecurity environment and the diverse composition of the DIB partnership. Three branches constitute XOP:

1. **Assess Branch:** Performs analysis of cybersecurity processes of DIB partners through the Cyber Resilience Analysis (CRA) tool. This branch also evaluates other vulnerability and penetration testing assessment procedures and provides them as a service to the DIB Partnership.
2. **Assist Branch:** Evaluates different cybersecurity technologies that can be provided to the DIB partnership as a pilot. Once the pilot is offered to the DIB, the information gathered from the capability is passed on to AD to determine if the information is applicable. Once the pilot is completed, and if it is determined to be successful, it may be considered as a permanent service offering for the Partnership.
3. **Architect Branch:** Researches and identifies the most effective ways to communicate with the DIB partnership. Their research discovers technologies that can best support transmitting cyber threat information from AD to the Partnership.

Mission Support Division (MSD): MSD executes functional areas including internal/external customer services, outreach, operational metrics, process improvement, quality assurance, quality control and organizational training. MSD builds and manages relationships with a wide range of DIB companies and USG stakeholders, and drives special projects that improve the overall customer experience. MSD is comprised of two branches:

1. **Customer Engagement:** Focused on building strong customer relationships to support the needs of the DIB; DIB Partner onboarding and training; curating events including Technical Exchanges, Regional Partner Exchanges, web conferences, panel discussions; and facilitating Analyst-to-Analyst, Business-to-Business, Government-to-Government Exchanges.
2. **Organizational Readiness:** A team of knowledge managers, business and process analysts; quality control analysts; quality assurance analysts, training managers, process owners and support staff to drive continual process improvement. Systematically coordinates and aligns resources and functions with the DCISE vision, mission, goals and objectives through the DCISE Performance Management Plan.

Pub. Date 4 NOV 2021